

1 90. (New) A digital signature process as recited in claim 57 wherein each of said distinct
2 random prime number has the same number of bits.

1 91. (New) A digital signature system as recited in claim 62 wherein said step of solving said
2 sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of
3 exponentiator units operating substantially simultaneously.

1 92. (New) A digital signature system as recited in claim 62 wherein each of said distinct
2 random prime number has the same number of bits.

REMARKS

This amendment is being submitted along with a Request for Continued Examination (RCE) under 37 CFR 1.114 for the above identified prior application. Please consider the above recited amendments to the claims and the following remarks in response to the Final Office Action mailed on December 26, 2000 for the above identified prior application.

Claims 14 - 92 are now pending. Claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 have been amended to more particularly point out subject matter which the Applicants regard as their invention. New claims 67 through 92 have been added. Support for the new claims 67 through 92 and for the amendments to claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 is found in the specification of the originally filed application. No new subject matter has been added.

I. Non-Statutory Double Patenting Rejections:

Claims 14 through 66 have been rejected in the above referenced Office Action under the judicially created doctrine of double patenting over claims 1 through 13 of U.S. Patent No. 5,848,159 (heretofore referred to as the issued patent). Filed herewith is a terminal disclaimer under 37 CFR 1.321(c) disclaiming the term of this patent subsequent to the date of expiration of U.S. Patent No. 5,848,159, filed January 16, 1997. Therefore, Applicants request that the rejection under the judicially created doctrine of double patenting be withdrawn.

II. Rejections Under 35 U.S.C. § 103(a):

Claims 14-66 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Kawamura et al. (U.S. Patent No. 5,046,094) in view of Menezes et al. (pp. 89, 612, and 613 of the Handbook of Applied Cryptography).

Based on all of the same arguments and reasoning submitted in Applicants' response to the previous Office Action mailed on April 27, 2000, Applicants respectfully maintain that neither Kawamura et al. nor Menezes et al., taken individually or collectively, teaches a "multi-prime" cryptographic scheme using a composite number n having more than two primes as recited in independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present

application. Therefore, Applicants maintain that independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application are patentable under 35 U.S.C. § 103(a) over Kawamura et al. in view of Menezes et al. Claims 18-21, 23-26, 28-31, 33-36, 38-41, 43-46, 48-51, 53-56, 58-61, 63-66, 68-71, and 73-66 depend from patentable claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 respectively, and as such include all of the limitations of patentable claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 rendering them patentable also.

Claims 67-68, 69-70, 71-72, 73-74, 75-76, 77-78, 79-80, 81-82, 83-84, 85-86, 87-88, 89-90, and 91-92 depend from patentable claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 respectively, and as such include all of the limitations of patentable claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 rendering them patentable also.

III. Summary of Interview with Examiner:

On January 16, 2001, Applicants Attorney Justin Boyce and Examiner Jeffrey J. Leaning discussed the above referenced patent application via telephone. The interview focused on issues including: (1) whether Menezes et al. teaches a multi-prime cryptographic scheme using a composite number n having more than two primes; and (2) whether Kawamura et al. teaches an application of the Chinese Remainder Theorem to a conventional cryptographic scheme using two primes that is equivalent to the application of the Chinese Remainder Theorem to the “multi-prime” cryptographic scheme of the present invention.

During the interview, Applicants Attorney further explained the arguments supporting the Applicants’ assertion that neither Kawamura et al. nor Menezes et al., taken individually or collectively, teaches a “multi-prime” cryptographic scheme using a composite number n having more than two primes as recited in independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application. Applicants Attorney elaborated verbally on all of the arguments and reasoning submitted in Applicants’ response to the previous Office Action mailed on April 27, 2000.

In response to the comments of Applicants Attorney (highlighting portions of the arguments submitted in Applicants’ response to the previous Office Action mailed on April 127, 2000), the Examiner agreed with the fact that the Chinese Remainder Theorem (CRT) is an existence proof that does not provide any actual solutions, but merely states that a solution must exist for solving a system of multiple linear congruencies under certain conditions. The Examiner further stated that he was unaware that there are many different types of Chinese Remainder Algorithms which may be applied to solve a system of multiple linear congruencies. However, the Examiner stated that he would take the position that it would be obvious to derive the particular Chinese Remainder Algorithm solutions recited in the claims of the present application based on Chinese Remainder Algorithms previously applied to two prime RSA encryption schemes. The Examiner said that he would research the issue further to find specific references teaching the application of Chinese Remainder Algorithms to two-prime RSA encryption schemes and/or references teaching the application of Chinese Remainder Algorithms to solve systems of multiple linear congruencies other than those used in RSA encryption schemes.

After discussing the Menezes et al. reference, the Examiner stated that he has found other references which he believes to better teach a multi-prime cryptographic scheme using a composite number n having more than two primes. Specifically, the Examiner stated that he was

prepared to cite Rivest et al. (U.S. Patent Application No. 4,405,829) and/or Slavin (U.S. Patent Application No. 5,974,151) as teaching a multi-prime cryptographic scheme using a composite number n having more than two primes. However, the Examiner was not at prepared at the time of the interview to point out all portions of each of these references which the Examiner believes to teach associated claimed elements of the present invention.

IV. Each of the amended independent claims is patentable over all of the cited references because none of the cited references teaches a system or method "... for establishing cryptographic communications that are backwards compatible with preexisting public key infrastructures ... wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater than 2, ... [and] ... p_1, p_2, \dots, p_k are distinct random prime numbers"

Applicants respectfully submit that neither Kawamura et al. nor Menezes et al., taken individually or collectively, teaches a "multi-prime" cryptographic scheme "wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater than 2, ... [and] ... p_1, p_2, \dots, p_k are distinct random prime numbers" as recited in the amended independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application.

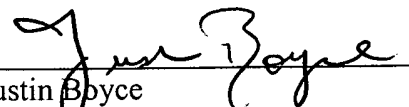
Applicants also respectfully submit that neither Rivest et al. nor Slavin, taken individually or collectively, teaches a "multi-prime" cryptographic scheme "wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater than 2, ... [and] ... p_1, p_2, \dots, p_k are distinct random prime numbers" as recited in the amended independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application.

Applicants respectfully request that the Examiner cite all prior art references that the Examiner considers to be closest to the present invention. Furthermore, Applicants request that the Examiner point out all portions of each prior art reference which the Examiner believes to teach associated claimed elements of the present invention.

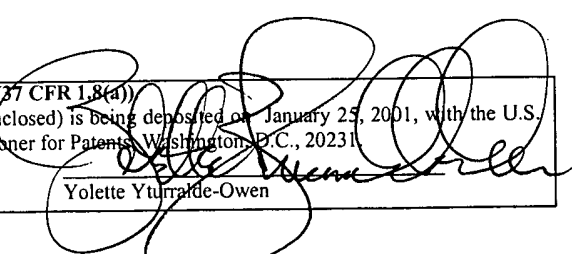
In view of the foregoing amendments and remarks, it is submitted that the application is now in condition for allowance and a notice of allowance of the pending claims 14 through 92 is respectfully requested. In the event that a telephone conference would expedite prosecution of the application, the Examiner is respectfully invited to contact the undersigned by telephone at the number set out below.

Respectfully submitted,

Dated: January 25, 2001
OPPENHEIMER WOLFF & DONNELLY LLP
Customer No. 25696
1400 Page Mill Road
Palo Alto, California 94304
Tel: (650) 320-4000
Fax: (650) 320-4100


Justin Boyce
Reg. No. 40,920

CERTIFICATE OF MAILING (37 CFR 1.8(a))
I hereby certify that this paper (along with any referred to as being attached or enclosed) is being deposited on January 25, 2001, with the U.S. Postal Service as First class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C., 20231.
Date: January 25, 2001


Yvette Yturralde-Owen